

I claim:

1. A method for determination of a end state, which has n bits and is iterated N times, of a shift register arrangement from a given initial state, which has n bits, of the shift register arrangement, with the iteration rule for the shift register arrangement being given by the characteristic polynomial

$$f(x) = 1 + c_1 \cdot x + c_2 \cdot x^2 + \dots + c_{n-1} \cdot x^{n-1} + x^n$$

where  $c_1, c_2, \dots, c_{n-1} \in \{0;1\}$ , comprising the following steps:

a) determining the polynomial

$$f^*(x) = 1 + c_{n-1} \cdot x + c_{n-2} \cdot x^2 + \dots + x^n$$

by reflecting of the coefficients of the polynomial

$$f(x) = 1 + c_1 \cdot x + c_2 \cdot x^2 + \dots + c_{n-1} \cdot x^{n-1} + x^n;$$

b) for  $j = 1, \dots, n$ , determining that representative of the remaining class

$$\left[ x^{N+j-1} \right] \bmod f^*,$$

whose degree is less than n;

c) multiplying the bit sequence of the initial state by a matrix whose j-th row or j-th column for  $j=1, \dots, n$  is given by the coefficients of the representative of the remaining class

$$\left[ x^{N+j-1} \right] \bmod f^*$$

as determined in step b).

2. The method as claimed in claim 1, wherein the representatives of the remaining classes

$$\left[ x^N \right] \bmod f^*, \left[ x^{N+1} \right] \bmod f^*, \dots \left[ x^{N+n-1} \right] \bmod f^*$$

are each calculated explicitly by means of a suitable algorithm, in particular by means of a square and multiply algorithm.

3. The method as claimed in claim 1, wherein only the representative of the remaining class

$$\left[ x^N \right] \bmod f^*$$

is calculated explicitly by means of a suitable algorithm, in particular by means of a square and multiply algorithm, and in that the representatives of the remaining classes

$$\left[ x^{N+j-1} \right] \bmod f^*$$

where  $j=2, \dots, n$  are obtained by  $(n-1)$  calculated iterations from the coefficients of the representative of the remaining class

$$\left[ x^N \right] \bmod f^*.$$

4. The method as claimed in claim 3, wherein the representatives of the remaining classes

$$\left[ x^{N+j-1} \right] \bmod f^*$$

where  $j=2, \dots, n$  are obtained by  $(n-1)$  calculated iterations of a shift register arrangement of the MSRG type from the coefficients of the representative of the remaining class

$$\left[ x^N \right] \bmod f^*$$

where the iteration rule for the shift register arrangement is given by the characteristic polynomial

$$f^*(x) = 1 + c_{n-1} \cdot x + c_{n-2} \cdot x^2 + \dots + x^n.$$

5. The method as claimed in claim 1, wherein the end state, which has n bits and is iterated N times, is used as an initialization state for the production of a pseudo-noise sequence which is shifted through N bits.

6. The method as claimed in claim 1, wherein the end state, which has n bits and is iterated N times, is written as the initialization state to a shift register arrangement which comprises n shift register cells.

7. The method as claimed in claim 6, wherein the shift register arrangement is a shift register arrangement of the SSRG type which comprises n shift register cells and whose structure is given by the characteristic polynomial

$$f(x) = 1 + c_1 \cdot x + c_2 \cdot x^2 + \dots + c_{n-1} \cdot x^{n-1} + x^n.$$

8. The method as claimed in claim 1, wherein the method is used in order to produce a spreading sequence with an offset of N bits in CDMA transmission systems, in particular CDMA transmission systems based on the UMTS or IS-95 transmission standards.

9. The method as claimed in claim 8, wherein the method is used for production of the scrambling codes which are defined in the UMTS standard.

10. The method as claimed in claim 8, wherein the spreading sequence is used for transmitter-end spread coding of the transmitted signals.

11. The method as claimed in claim 8, wherein the spreading sequence is used for receiver-end decoding of the received signals.

12. The method as claimed in claim 8, wherein the spread coding is started in the CDMA transmission system at a different time than the signal transmission, with the end state, which has  $n$  bits and is iterated  $N$  times, being used as the initialization state for the production of the time-shifted spreading sequence.

13. The method as claimed in claim 8, wherein a given code number defines the offset of a spreading sequence, with the end state, which has  $n$  bits and is iterated  $N$  times, being used as the initialization state for the production of the spreading sequence which is associated with the code number  $N$ .

14. An apparatus for determination of an end state, which has n bits and is iterated N times, of a shift register arrangement from a given initial state, which has n bits, of the shift register arrangement, with the iteration rule for the shift register arrangement being given by the characteristic polynomial

$$f(x) = 1 + c_1 \cdot x + c_2 \cdot x^2 + \dots + c_{n-1} \cdot x^{n-1} + x^n$$

where  $c_1, c_2, \dots, c_{n-1} \in \{0;1\}$ , comprising:

- means for determination of the polynomial

$$f^*(x) = 1 + c_{n-1} \cdot x + c_{n-2} \cdot x^2 + \dots + x^n$$

by reflecting of the coefficients of the polynomial

$$f(x) = 1 + c_1 \cdot x + c_2 \cdot x^2 + \dots + c_{n-1} \cdot x^{n-1} + x^n;$$

- means for remaining class determination and, for  $j=1, \dots, n$ , in each case determine that representative of the remaining class

$$\left[ x^{N+j-1} \right]_{\text{mod } f^*}$$

whose degree is less than n; and

- means for multiplication of the bit sequence of the initial state by a matrix whose j-th row or j-th column for  $j=1, \dots, n$  is given by the coefficients of the representative of the remaining class

$$\left[ x^{N+j-1} \right]_{\text{mod } f^*},$$

whose degree is less than n.

15. The apparatus as claimed in claim 14, wherein the means for remaining class determination in each case explicitly calculate the representatives of the remaining classes

$$\left[ x^N \right] \bmod f^*, \left[ x^{N+1} \right] \bmod f^*, \dots \left[ x^{N+n-1} \right] \bmod f^*$$

by means of a suitable algorithm, in particular by means of a square and multiply algorithm.

16. The apparatus as claimed in claim 14, wherein the means for remaining class determination explicitly calculate only the representative of the remaining class

$$\left[ x^N \right] \bmod f^*$$

by means of a suitable algorithm, in particular by means of a square and multiply algorithm, and in that the means for remaining class determination obtain the representatives of the remaining classes

$$\left[ x^{N+j-1} \right] \bmod f^*$$

where  $j=2, \dots, n$  by  $(n-1)$  calculated iterations from the coefficients of the representative of the remaining class

$$\left[ x^N \right] \bmod f^*.$$

17. The apparatus as claimed in claim 16, wherein the means for remaining class determination obtain the representatives of the remaining classes

$$\left[ x^{N+j-1} \right] \bmod f^*$$

where  $j=2, \dots, n$  by  $(n-1)$  calculated iterations of a shift register arrangement of the MSRG type from the coefficients of the representative of the remaining class

$$\left[ x^N \right]_{\text{mod } f^*}$$

where the iteration rule for the shift register arrangement is given by the characteristic polynomial

$$f^*(x) = 1 + c_{n-1} \cdot x + c_{n-2} \cdot x^2 + \dots + x^n.$$

18. The apparatus as claimed in claim 14, wherein the apparatus for determination of an end state, which has n bits and is iterated N times, writes the end state as the initialization state in a shift register arrangement comprising n shift register cells.

19. The apparatus as claimed in claim 18, wherein the shift register arrangement is a shift register arrangement of the SSRG type which comprises n shift register cells  $(R_1, R_2, \dots, R_n)$  and whose structure is given by the characteristic polynomial

$$f(x) = 1 + c_1 \cdot x + c_2 \cdot x^2 + \dots + c_{n-1} \cdot x^{n-1} + x^n.$$

20. The use of an apparatus as claimed in claim 14 for production of a spreading sequence with an offset with N bits in a CDMA transmission system, in particular in a CDMA transmission system corresponding to one of the transmission standards UMTS or IS-95.

21. The use as claimed in claim 20, wherein the spreading sequence is used for transmitter-end spread coding of the signals to be transmitted.

22. The use as claimed in claim 20, wherein the spreading sequence is used for receiver-end decoding of the received signals.

23. The use as claimed in claim 20, wherein the spread coding is started in the CDMA transmission system at a different time than the signal transmission, with the end state, which has n bits and is iterated N times, being used as the initialization state for the production of the time-shifted spreading sequence.

24. The use as claimed in claim 20, wherein a given code number defines the offset of a spreading sequence, with the end state, which has  $n$  bits and is iterated  $N$  times, being used as the initialization state for the production of the spreading sequence which is associated with the code number  $N$ .